

# New Quadriphase Sequences families with Larger Linear Span and Size

Wenping Ma

National Key Lab. of ISN, Xidian University, Xi'an 710071, P.R.China  
wp\_ma@mail.xidian.edu.cn

**Abstract.** In this paper, new families of quadriphase sequences with larger linear span and size have been proposed and studied. In particular, a new family of quadriphase sequences of period  $2^n - 1$  for a positive integer  $n = em$  with an even positive factor  $m$  is presented, the cross-correlation function among these sequences has been explicitly calculated. Another new family of quadriphase sequences of period  $2(2^n - 1)$  for a positive integer  $n = em$  with an even positive factor  $m$  is also presented, a detailed analysis of the cross-correlation function of proposed sequences has also been presented.

## 1 Introduction

Family of pseudorandom sequences with low cross correlaton and large linear span has important application in code-division multiple access communications and cryptology. Quadriphase sequences are the one most often used in practice because of their easy implementation in modulators. However, up to now, only few families of optimal quadriphase sequences are found [1],[5,6,7,8,9,10,11,12].

Among the known optimal quadriphase sequence families, the most famous ones are the families  $\mathcal{A}$  and  $\mathcal{B}$  investigated by Boztas, Hammons, and Kumar in [5]. The family  $\mathcal{A}$  has period  $2^n - 1$  and family size  $2^n + 1$ , while the two corresponding parameters of the family  $\mathcal{B}$  are  $2(2^n - 1)$  and  $2^{n-1}$ , respectively. Another optimal family  $\mathcal{C}$  was discussed in [10], and this family has the same correlation properties as the family  $\mathcal{B}$ . Families  $S(t)$  were defined by Kumar et. [6], and when  $t = 0$  or  $m$  is odd, the correlation distributions of families  $S(t)$  are established by Kai-Uwe Schmidt [7]. Tang, Udaya, and Fan generalized the family  $\mathcal{A}$  and proposed a new family of quadriphase sequences with low correlation in [12]. By utilizing a variation of family  $\mathcal{B}$  and  $\mathcal{C}$ , Tang and Udaya obtained the family  $\mathcal{D}$ , which has period  $2(2^n - 1)$  and a larger family size  $2^n$  [9]. Recently, Wenfeng Jiang, Lei Hu, Xiaohu Tang, and Xiangyong Zeng proposed two new families  $\mathcal{S}$  and  $\mathcal{U}$  of quadriphase sequences with larger linear spans for a positive integer  $n = em$  with an odd positive factor  $m$ . Both families are asymptotically optimal with respect to the Welch and Sidelnikov bounds. The family  $\mathcal{S}$  has period  $2^n - 1$ , family size  $2^n + 1$ , and maximum correlation magnitude  $2^{\frac{n}{2}} + 1$ . The family  $\mathcal{U}$  has period  $2(2^n - 1)$ , family size  $2^n$ , and maximum correlation magnitude  $2^{\frac{n+1}{2}} + 2$  [1].

In this paper, motivated by the constructions proposed in [1,2,3,4,6], the new families of quadriphase sequences with larger linear span and size have been presented. As a special case of the sequence families, a new family of quadriphase sequences of period  $2^n - 1$  for a positive integer  $n = em$  with an even positive factor  $m$  is presented, the cross-correlation function among these sequences has been explicitly calculated. Another new family of quadriphase sequences of period  $2(2^n - 1)$  for a positive integer  $n = em$  with an even positive factor  $m$  is also presented, a detailed analysis of the cross-correlation function of proposed sequences has been presented. The sequences have low correlations and are useful in code division multiple access communication systems and cryptography.

This paper is organized as follows. Section 2 introduces the preliminaries and notations. In section 3, we give the constructions and properties of the new sequences families  $\mathcal{L}$  and  $\mathcal{V}$  with period  $2^n - 1$ . The constructions and correlation properties of the new sequences family  $\mathcal{W}$  with period  $2(2^n - 1)$  are presented in section 4. The conclusions and acknowledgement are presented in section 5 and 6 respectively.

## 2 Preliminaries

### 2.1 Basic Concepts

Let  $a = \{a(t)\}$  and  $b = \{b(t)\}$  be two quadriphase sequences of period  $L$ , the correlation function  $R_{a,b}(\tau)$  between them at a shift  $0 \leq \tau \leq L - 1$  is defined by

$$R_{a,b}(\tau) = \sum_{t=0}^{L-1} \omega^{a(t)-b(t+\tau)}$$

where  $\omega^2 = -1$ .

Let  $\mathcal{F}$  be a family of  $M$  quadriphase sequences

$$\mathcal{F} = \{a_i = \{a(t)\} : 1 \leq i \leq M\}.$$

The maximum correlation magnitude  $R_{max}$  of  $\mathcal{F}$  is

$$R_{max} = \max\{|R_{a_i,a_j}(\tau)| : 1 \leq i, j \leq M, \ i \neq j \text{ or } \tau \neq 0\}.$$

### 2.2 Galois Ring

Let  $Z_4[x]$  be the ring of all polynomials over  $Z_4$ . A monic polynomial  $f(x) \in Z_4[x]$  is said to be basic primitive if its projection  $\overline{f(x)}$

$$\overline{f(x)} = f(x) \text{ mod } 2$$

is primitive over  $Z_2[x]$ .

Let  $f(x)$  be a basic primitive polynomial of degree  $n$  over  $Z_4$ , and  $Z_4[x]/(f(x))$  denotes the ring of residue classes of polynomials over  $Z_4$  modulo  $f(x)$ . It can be

shown that this quotient ring is a commutative ring with identity called Galois ring, denoted as  $GR(4, n)$ [11]. As a multiplicative group, the units  $GR^*(4, n)$  have the following structure:

$$GR^*(4, n) = G_A \otimes G_C$$

where  $G_C$  is a cyclic group of order  $2^n - 1$  and  $G_A$  is an Abelian group of order  $2^n$ . Naturally, the projection map  $\bar{a}$  from  $Z_4$  to  $Z_2$  induces a homomorphism from  $GR(4, n)$  to finite field  $GF(2^n)$ .

Let  $\beta \in GR^*(4, n)$  be a generator of the cyclic group  $G_C$ , then  $\alpha = \bar{\beta}$  is a primitive root of  $GF(2^n)$  with primitive polynomial  $\bar{f}(x)$  over  $Z_2$ .

For each element  $x \in GR(4, n)$  has a unique 2-adic representation of the form

$$x = x_0 + 2x_1, x_0, x_1 \in G_C. \quad (1)$$

Let  $n = em$ , The *Frobenius* automorphism of  $GR(4, n)$  over  $GR(4, e)$  is given by

$$\sigma(x) = x_0^{2^e} + 2x_1^{2^e}$$

for any element  $x$  expressed as (1), and the trace function  $Tr_e^n$  from  $GR(4, n)$  to  $GR(4, e)$  is defined by

$$Tr_e^n(x) = x + \sigma(x) + \sigma^2(x) + \cdots + \sigma^{m-1}(x)$$

where  $\sigma^i(x) = \sigma^{i-1}(\sigma(x))$  for  $1 < i \leq m - 1$ .

Let  $GF(q)$  is the finite field with  $q$  elements,  $tr_e^n(x)$  is the trace function from  $GF(2^n)$  to  $GF(2^e)$ , i.e.,

$$tr_e^n(x) = x + x^{2^e} + \cdots = x^{2^{e(\frac{n}{e}-1)}}, x \in GF(2^n).$$

We have  $\overline{Tr_e^n(x)} = tr_e^n(\bar{x})$ , where  $x \in GR(4, n)$ .

Throughout this paper, we suppose (1)  $n = em$  with  $e \geq 2$  and  $m \geq 2$ , (2)  $\lambda \in GR(4, e)$  such that  $\bar{\lambda} \in GF(2^e) \setminus \{1, 0\}$ .

### 2.3 Linear Span

Let

$$f(x) = Tr_1^n[(1 + 2\alpha)x] + 2 \sum_{i=1}^r Tr_1^{n_i}(A_i x^{v_i}), \alpha \in G_C, A_i \in GF(2^{n_i}), x \in G_C,$$

where  $v_i$  is a coset leader of a cyclotomic coset modulo  $2^{n_i} - 1$ , and  $n_i | n$  is the size of the cyclotomic coset containing  $v_i$ . For sequence  $a = \{a_i\}$  such that

$$a_i = f(\beta), i = 0, 1, 2, \dots$$

where  $\beta$  is a primitive element of  $G_C$ .

Linear span of a sequence  $a$  is equal to  $n + \sum_{i, A_i \neq 0} n_i$ , or equivalently, the degree of the shortest linear feedback shift register that can generates  $a$  [1,4].

### 3 New Quadriphase Sequences with Larger Size and Linear Span

Define a function  $P(x)$  over  $GR(4, n)$  as

$$P(x) = \begin{cases} \sum_{j=1}^{l-1} Tr_1^n(x^{2^{ej}+1}) + Tr_1^{le}(x^{2^{le}+1}), & \text{if } m = 2l, \\ \sum_{j=1}^l Tr_1^n(x^{2^{ej}+1}), & \text{if } m = 2l + 1. \end{cases}$$

For any  $x, y \in GR(4, n)$ , it is easy to check that [1,2,3]

$$2P(x) + 2P(y) + 2P(x + y) = 2Tr_1^n[y(x + Tr_e^n(x))]. \quad (2)$$

**Definition 1.** Let  $\rho$  be an integer such that  $1 \leq \rho < \lfloor \frac{n}{2} \rfloor$ , a family of quaternary sequences of period  $2^n - 1$ ,  $\mathcal{L} = \{s_i(t) : 0 \leq t < 2^n - 1, 1 \leq i \leq 2^{\rho n} + 1\}$  is defined by

$$s_i(t) = \begin{cases} Tr_1^n[(1 + 2\lambda_0^i)\beta^t] + 2\sum_{k=1}^{\rho-1} Tr_1^n(\lambda_k^i \beta^{t(1+2^k)}) + 2P(\lambda\beta^t), & 1 \leq i \leq 2^{\rho n}, \\ 2Tr_1^n(\beta^t), & i = 2^{\rho n} + 1 \end{cases}$$

where  $\{(\lambda_0^i, \lambda_1^i, \dots, \lambda_{\rho-1}^i), i = 1, 2, \dots, 2^{\rho n}\}$  is an enumeration of the elements of  $G_C \times G_C \times \dots \times G_C$ ,  $\beta$  is a generator element of group  $G_C$ .

**Lemma 1.** All sequence in  $\mathcal{L}$  are cyclically distinct. Thus, the family size of  $\mathcal{L}$  is  $2^{n\rho} + 1$ .

*Proof.* The proof of lemma 1 is similar to the proofs of Lemma 1 and Lemma 6 in [4], we cancel the details.

#### 3.1 The Correlation Function of the Sequence Family

(1) Suppose  $s_i, s_j, 1 \leq i, j \leq 2^{\rho n}$ , are two sequences, the correlation function between  $s_i$  and  $s_j$  is

$$R_{s_i, s_j}(\tau) = \sum_{x \in G_C} \omega^{Tr_1^n[(1+2\gamma_0^i - (1+2\gamma_0^j)\delta)x] + 2\sum_{k=1}^{\rho-1} Tr_1^n(\eta_k x^{1+2^k}) + 2(P(\lambda x) + P(\lambda \delta x))} - 1 \quad (3)$$

where  $\delta = \beta^\tau$ ,  $\tau \neq 0$ ,  $\lambda_k^i - \delta^{1+2^k} \lambda_k^j = \eta_k, k = 1, 2, \dots, \rho - 1$ .

$$\begin{aligned}
& (R_{s_i, s_j}(\tau) + 1)(R_{s_i, s_j}(\tau) + 1)^* \\
&= \sum_{s \in G_C} \sum_{y \in G_C} \omega^{Tr_1^n[(1+2\gamma_0^i - (1+2\gamma_0^j)\delta)x + 2 \sum_{k=1}^{\rho-1} Tr_1^n(\eta_k x^{1+2^k}) + 2(P(\lambda x) + P(\lambda \delta x))]} \\
&\quad \cdot \omega^{-Tr_1^n[(1+2\gamma_0^i - (1+2\gamma_0^j)\delta)y + 2 \sum_{k=1}^{\rho-1} Tr_1^n(\eta_k y^{1+2^k}) + 2(P(\lambda y) + P(\lambda \delta y))]} \\
&= \sum_{x \in G_C} \sum_{y \in G_C} \omega^{Tr_1^n((1+2\gamma_0^i - (1+2\gamma_0^j)\delta)(x+3y))} \\
&\quad \cdot \omega^{2[\sum_{k=1}^{\rho-1} Tr_1^n[\eta_k(x^{1+2^k} + y^{1+2^k})] + P(\lambda x) + P(\lambda \delta x) + P(\lambda y) + P(\lambda \delta y)]} \\
&= \sum_{x \in G_C} \sum_{y \in G_C} \omega^{Tr_1^n((\Delta(x+3y)) + 2[\sum_{k=1}^{\rho-1} Tr_1^n[\eta_k(x^{1+2^k} + y^{1+2^k})] + P(\lambda x) + P(\lambda \delta x) + P(\lambda y) + P(\lambda \delta y))} \\
&= \sum_{z \in G_C} \sum_{y \in G_C} \omega^{Tr_1^n(\Delta z) + 2[\sum_{k=1}^{\rho-1} Tr_1^n[\eta_k((y+z+2\sqrt{yz})^{1+2^k} + y^{1+2^k})] + 2Tr_1^n(\Delta\sqrt{yz})} \\
&\quad \cdot \omega^{2P(\lambda(y+z+2\sqrt{yz})) + 2P(\lambda \delta(y+z+2\sqrt{yz})) + 2P(\lambda y) + 2P(\lambda \delta y)]} \\
&= \sum_{z \in G_C} \omega^{\phi(z)} \sum_{y \in G_C} \omega^{2[Tr_1^n(y(\Delta^2 z)) + v(y, z)]}
\end{aligned}$$

where  $\Delta = 1 + 2\gamma_0^i - (1 + 2\gamma_0^j)\delta$ ,  $x = y + z + 2\sqrt{yz}$ ,

$$\phi(z) = Tr_1^n(\Delta z) + 2[P(\lambda z) + 2P(\lambda \delta z)] + 2 \sum_{k=1}^{\rho-1} Tr_1^n(\eta_k z^{1+2^k}),$$

$$v(y, z) = \sum_{k=1}^{\rho-1} Tr_1^n[\eta_k((y+z+2\sqrt{yz})^{1+2^k} + y^{1+2^k} + z^{1+2^k})] + P(\lambda(y+z+2\sqrt{yz})) + P(\lambda \delta(y+z+2\sqrt{yz})) + P(\lambda y) + P(\lambda \delta z) + P(\lambda z) + P(\lambda \delta z).$$

Then, by (2), we have

$$\begin{aligned}
2v(y, z) &= 2Tr_1^n[\lambda y(\lambda z + Tr_e^n(\lambda z)) + \lambda \delta y(\lambda \delta z + Tr_e^n(\lambda \delta z))] + 2Tr_1^n \sum_{k=1}^{\rho-1} [\eta_k(z y^{2^k} + z^{2^k} y)] \\
&= 2Tr_1^n[y(\lambda^2 z + \lambda Tr_e^n(\lambda z) + \lambda^2 \delta^2 z + \lambda \delta Tr_e^n(\lambda \delta z)) + \sum_{k=1}^{\rho-1} (\eta_k^{-2^k} z^{-2^k} + \eta_k z^{2^k})].
\end{aligned}$$

Define

$$L(z) = \bar{\delta} tr_e^n(\bar{\delta} z) + tr_e^n(z) + \frac{1}{\bar{\lambda}^2} (\bar{\lambda}^2 + 1)(\bar{\delta}^2 + 1)z + \frac{1}{\bar{\lambda}^2} \sum_{k=1}^{\rho-1} (\bar{\eta}_k^{-2^k} z^{-2^k} + \bar{\eta}_k z^{2^k}), \quad (4)$$

where  $z \in GF(2^n)$ , then  $L(z)$  is a linear equation over  $GF(2^n)$ .

For  $L(z) = 0$ , we have to count the number of solutions in the equation

$$\bar{\delta} tr_e^n(\bar{\delta} z) + tr_e^n(z) + \frac{1}{\bar{\lambda}^2}(\bar{\lambda}^2 + 1)(\bar{\delta}^2 + 1)z + \frac{1}{\bar{\lambda}^2} \sum_{k=1}^{\rho-1} (\bar{\eta}_k^{-2^k} z^{-2^k} + \bar{\eta}_k z^{2^k}) = 0 \quad (5)$$

for given  $\eta_i$ 's in  $G_C$ ,  $\lambda \in G_C$  such that  $\bar{\lambda} \in GF(2^e) \setminus \{0, 1\}$ , and  $\bar{\delta} \in GF(2^n) \setminus \{0\}$ .

It is easy to verify that  $\frac{1}{\bar{\lambda}^2}(\bar{\lambda}^2 + 1)(\bar{\delta}^2 + 1)z + \frac{1}{\bar{\lambda}^2} \sum_{k=1}^{\rho-1} (\bar{\eta}_k^{-2^k} z^{-2^k} + \bar{\eta}_k z^{2^k})$  is not a constant polynomial of  $z$ , and the maximum number of solutions of equation  $L(z) = 0$  is at most  $2^{2(\rho-1)+2e}$ . Thus

$$|R_{s_i, s_j}(\tau) + 1| \leq 2^{\frac{n+2(\rho-1)+2e}{2}}. \quad (6)$$

(2) If  $1 \leq i \leq 2^{\rho n}$  and  $j = 2^{\rho n} + 1$  are two sequences, then the correlation function between  $s_i$  and  $s_j$  is

$$R_{s_i, s_j}(\tau) = \sum_{x \in G_C} \omega^{Tr_1^n[(1+2\gamma_1-2\delta)x] + 2 \sum_{k=1}^{\rho-1} Tr_1^n(\lambda_k^i x^{1+2^k}) + 2P(\lambda x)} - 1,$$

similar to analysis above, the equation (4) become the following equation.

$$L(z) = \frac{1 + \bar{\lambda}^2}{\bar{\lambda}^2} z + tr_e^n(z) + \frac{1}{\bar{\lambda}^2} \sum_{k=1}^{\rho-1} ((\bar{\lambda}_k^i)^{-2^k} z^{-2^k} + \bar{\lambda}_k^i z^{2^k}).$$

Thus

$$|R_{s_i, s_j}(\tau) + 1| \leq 2^{\frac{n+2(\rho-1)+e}{2}}. \quad (7)$$

(3) If  $i = j = 2^{\rho n} + 1$ , then  $s_i$  is essentially a binary  $m$ -sequence, Then  $R_{s_i, s_j}(\tau) = -1$  for  $\tau \neq 0$ .

(4) Suppose that  $s_i, s_j$ ,  $1 \leq i, j \leq 2^{\rho n}$ , are two sequences, then

$$R_{s_i, s_j}(0) = \sum_{x \in T} \omega^{2Tr_1^n[(\gamma_0^i + \gamma_0^j)x] + 2 \sum_{k=1}^{\rho-1} Tr_1^n(\eta_k x^{1+2^k})} - 1,$$

similar to the analysis above, we have

$$|R_{s_i, s_j}(0) + 1| \leq 2^{\frac{n+2(\rho-1)}{2}}. \quad (8)$$

It seems difficult to get tighter bound for inequality(6)-(8), thus we propose the following open problem.

**Open problem:** For  $n = em$ , how many solutions exist exactly for the equation (5) over finite field  $GF(2^n)$ .

Following the discussion above, we have the following theorem.

**Theorem 1.** For  $n = em$  and an integer  $\rho$  such that  $1 \leq \rho < \lfloor \frac{n}{2} \rfloor$ , the proposed quadriphase family has  $2^{\rho n} + 1$  cyclically distinct binary sequences of period  $2^n - 1$ . The maximum correlation magnitude of sequences is smaller than  $1 + 2^{\frac{n+2(\rho-1)+2e}{2}}$ . Therefore, the sequences family constitutes a  $(2^n - 1, 2^{\rho n} + 1, 1 + 2^{\frac{n+2(\rho-1)+2e}{2}})$  quadriphase signal set.

### 3.2 Linear Spans of the Sequence

In order to express clearly, let

$$s(\lambda_0, A, t) = Tr_1^n[(1 + 2\lambda_0)\beta^t] + 2 \sum_{k=1}^{\rho-1} Tr_1^n(\lambda_k \beta^{t(1+2^k)}) + 2P(\lambda\beta^t),$$

where  $A = (\lambda_1, \dots, \lambda_{\rho-1})$ .

We divide the set  $\Delta = \{1, 2, \dots, \rho-1\}$  into two sets  $A$  and  $B$  such that  $\Delta = A \cup B$ , where  $A = \{ke + r : 1 \leq k \leq \lfloor \frac{\rho-1}{e} \rfloor, 0 < r < e\}$ ,  $B = \{ke : 1 \leq k \leq \lfloor \frac{\rho-1}{e} \rfloor\}$ .

**Theorem 2.** (1) Consider a sequence represented by  $s(\lambda_0, A, t)$  where  $j$   $\lambda_i$ 's with  $i \in A$  in  $A = (\lambda_1, \dots, \lambda_{\rho-1})$  are equal to 0 and  $l$   $\lambda_i$ 's with  $i \in B$  in  $A = (\lambda_1, \dots, \lambda_{\rho-1})$  are equal to  $\bar{\lambda}$ . Let  $LS_{j,l}(\rho)$  be the linear span of the sequence. Then

$$LS_{j,l}(\rho) = n(\frac{m-1}{2} + \rho - 1 - \lfloor \frac{\rho-1}{e} \rfloor + 1 - j - l), 0 \leq j \leq |A|, 0 \leq l \leq |B|.$$

and there are  $\binom{\rho-1-\lfloor \frac{\rho-1}{e} \rfloor}{j} \binom{\lfloor \frac{\rho-1}{e} \rfloor}{l} 2^n (2^n - 1)^{\rho-1-j-l}$  sequences having linear span  $LS_{j,l}(\rho)$ .

(2) The linear span of the sequences  $s_{2^n\rho+1}(t)$  is  $n$ .

*Proof.* First, consider the linear span of sequences with  $m$  is odd. A sequence constructed above has a total of  $\frac{m-1}{2} + \rho - 1 - \lfloor \frac{\rho-1}{e} \rfloor + 1$  trace terms and each trace term has the linear span of  $n$ . If  $j$   $\lambda_i$ 's with  $i \in A$  in  $A = (\lambda_1, \dots, \lambda_{\rho-1})$  are equal to 0, and  $l$   $\lambda_i$ 's with  $i \in B$  in  $A = (\lambda_1, \dots, \lambda_{\rho-1})$  are equal to  $\bar{\lambda}^{2^i+1}$ , it has  $\frac{m-1}{2} + \rho - 1 - \lfloor \frac{\rho-1}{e} \rfloor + 1 - j - l$  nonzero trace terms and the corresponding linear span of the sequences is given by

$$LS_{j,l}(\rho) = n(\frac{m-1}{2} + \rho - 1 - \lfloor \frac{\rho-1}{e} \rfloor + 1 - j - l), 0 \leq j \leq |A|, 0 \leq l \leq |B|.$$

Since (1)  $j$   $\lambda_i$ 's with  $i \in A$  are 0 and  $(|A| - j)$   $\lambda_i$ 's are nonzero, (2)  $l$   $\lambda_i$ 's with  $i \in B$  are  $\bar{\lambda}^{2^i+1}$  and  $(|B| - l)$   $\lambda_i$ 's are not equal to  $\bar{\lambda}^{2^i+1}$ , (3) the number of  $\lambda_0$  is  $2^n$ . Therefore, the number of corresponding sequences given above is

$$\begin{aligned} & \binom{\rho-1-\lfloor \frac{\rho-1}{e} \rfloor}{j} (2^n - 1)^{\rho-1-\lfloor \frac{\rho-1}{e} \rfloor-j} \cdot \binom{\lfloor \frac{\rho-1}{e} \rfloor}{l} (2^n - 1)^{\lfloor \frac{\rho-1}{e} \rfloor-l} \cdot 2^n \\ &= \binom{\rho-1-\lfloor \frac{\rho-1}{e} \rfloor}{j} \cdot \binom{\lfloor \frac{\rho-1}{e} \rfloor}{l} 2^n (2^n - 1)^{\rho-1-l-j}. \end{aligned}$$

Applying this result to each  $j$  and each  $l$ , we obtain the linear span of the proposed sequence. Using a similar approach to the odd case, we see that the linear span of both sequences is same.

For the sequences families above, some special conditions had already been discussed, for example, the case with  $n = em$ , where  $m$  is an odd, and  $\rho = 1$  had been discussed in [1]. In the following, we will discuss another special case with  $n = em$ , where  $m$  is an even, and  $\rho = 1$ , we call this special sequence family as family  $\mathcal{V}$ .

### 3.3 Correlation Function of the Sequence family for even $m$ and $\rho = 1$

If  $\rho = 1$ , then the equation (5) becomes

$$\bar{\delta}Tr_e^n(\bar{\delta}z) + Tr_e^n(z) + \frac{(\bar{\lambda}^2 + 1)(\bar{\delta}^2 + 1)}{\bar{\lambda}^2}z = 0 \quad (9)$$

In the following, we study the solution of the equation (9).

Let  $Tr_e^n(\bar{\delta}z) = a$ ,  $Tr_e^n(z) = b$ , then

$$z = \frac{\bar{\lambda}^2}{\bar{\lambda}^2 + 1} \frac{\bar{\delta}a + b}{\bar{\delta}^2 + 1}.$$

By computing  $Tr_e^n(z)$  and  $Tr_e^n(\bar{\delta}z)$ , we have

$$\begin{cases} aTr_e^n(\frac{\bar{\delta}}{\bar{\delta}^2 + 1}) + b[Tr_e^n(\frac{1}{\bar{\delta}^2 + 1}) - \frac{\bar{\lambda}^2 + 1}{\bar{\lambda}^2}] = 0 \\ a[Tr_e^n(\frac{1}{\bar{\delta}^2 + 1}) - \frac{\bar{\lambda}^2 + 1}{\bar{\lambda}^2}] + bTr_e^n(\frac{\bar{\delta}}{\bar{\delta}^2 + 1}) = 0 \end{cases} \quad (10)$$

The determinant of corresponding coefficient matrix of (10) is equal to

$$\begin{aligned} & [Tr_e^n(\frac{1}{\bar{\delta}^2 + 1}) - \frac{\bar{\lambda}^2 + 1}{\bar{\lambda}^2}]^2 + [Tr_e^n(\frac{\bar{\delta}}{1 + \bar{\delta}})]^2 \\ &= (\frac{\bar{\lambda}^2 + 1}{\bar{\lambda}^2})^2 + [Tr_e^n(\frac{1}{1 + \bar{\delta}})]^2 \end{aligned}$$

(1) If  $Tr_e^n(\frac{1}{1 + \bar{\delta}}) \neq \frac{\bar{\lambda}^2 + 1}{\bar{\lambda}^2}$ , then the determinant of coefficient matrix (10) is not equal to zero, the equation (10) has unique solution  $a = 0$ ,  $b = 0$ , then  $z = 0$ .

(2) If  $Tr_e^n(\frac{1}{1 + \bar{\delta}}) = \frac{\bar{\lambda}^2 + 1}{\bar{\lambda}^2}$ , then the determinant of coefficient matrix (10) is equal to zero,

$$aTr_e^n(\frac{1}{\bar{\delta} + 1}) + aTr_e^n(\frac{1}{\bar{\delta}^2 + 1}) + b[Tr_e^n(\frac{1}{\bar{\delta}^2 + 1}) - \frac{\bar{\lambda}^2 + 1}{\bar{\lambda}^2}] = 0,$$



thus  $a = b$ , the equation (10) has  $2^e$  solutions, then  $z = \frac{\bar{\lambda}^2}{\bar{\lambda}^2 + 1} \frac{1}{\bar{\delta} + 1} a$ .

$$\begin{aligned}
2P(\bar{\lambda}z) + 2P(\bar{\lambda}\bar{\delta}z) &= 2 \sum_{j=1}^{l-1} Tr_1^n [(\bar{\lambda}z)^{2^{ej}+1} + (\bar{\lambda}\bar{\delta}z)^{2^{ej}+1}] + 2Tr_1^{le} [(\bar{\lambda}z)^{2^{le}+1} + (\bar{\lambda}\bar{\delta}z)^{2^{le}+1}] \\
&= 2 \sum_{j=1}^{l-1} Tr_1^n \left[ \left( \frac{\bar{\lambda}^3 a}{1 + \bar{\lambda}^2} \right)^{2^{ej}+1} \left( \frac{1}{1 + \bar{\delta}} \right)^{2^{ej}+1} + \left( \frac{\bar{\lambda}^3 a}{1 + \bar{\lambda}^2} \right)^{2^{ej}+1} \left( \frac{\bar{\delta}}{1 + \bar{\delta}} \right)^{2^{ej}+1} \right] \\
&\quad + 2Tr_1^{le} \left[ \left( \frac{\bar{\lambda}^3 a}{1 + \bar{\lambda}^2} \right)^{2^{le}+1} \left( \frac{1}{1 + \bar{\delta}} \right)^{2^{le}+1} + \left( \frac{\bar{\lambda}^3 a}{1 + \bar{\lambda}^2} \right)^{2^{le}+1} \left( \frac{\bar{\delta}}{1 + \bar{\delta}} \right)^{2^{le}+1} \right] \\
&= 2Tr_1^e \left\{ \left( \frac{\bar{\lambda}^3 a}{1 + \bar{\lambda}^2} \right)^2 \left[ \sum_{j=1}^{l-1} Tr_e^n \left[ \left( \frac{1}{1 + \bar{\delta}} \right)^{2^{ej}+1} + \left( \frac{\bar{\delta}}{1 + \bar{\delta}} \right)^{2^{ej}+1} \right] \right. \right. \\
&\quad \left. \left. + Tr_e^{le} \left[ \left( \frac{1}{1 + \bar{\delta}} \right)^{2^{le}+1} + \left( \frac{\bar{\delta}}{1 + \bar{\delta}} \right)^{2^{le}+1} \right] \right] \right\} \\
&= 2Tr_1^e \left[ \left( \frac{\bar{\lambda}^3 a}{1 + \bar{\lambda}^2} \right)^2 (Tr_e^{le} 1 + Tr_e^n \left( \frac{1}{1 + \bar{\delta}} \right)) \right] \\
&= \begin{cases} 2Tr_1^n \left( \frac{\bar{\lambda}^2 z}{1 + \bar{\lambda}^2} \right), & \text{for odd } l, \\ 2Tr_1^n \left( \frac{\bar{\lambda}^2 z}{1 + \bar{\lambda}^2} \right), & \text{for even } l. \end{cases}
\end{aligned}$$

Thus,  $\phi(z) = Tr_1^n(\Delta z) + 2[P(\lambda z) + P(\lambda \bar{\delta} z)]$

$$= \begin{cases} 2Tr_1^n \left[ (\bar{\gamma}_0^i + (\bar{\gamma}_0^j + 1)\bar{\delta} + \frac{\bar{\lambda}^2}{1 + \bar{\lambda}^2})z \right], & \text{for odd } l, \\ 2Tr_1^n \left[ (\bar{\gamma}_0^i + (\bar{\gamma}_0^j + 1)\bar{\delta} + \frac{\bar{\lambda}^2}{1 + \bar{\lambda}^2})z \right], & \text{for even } l. \end{cases}$$

Because the solutions space of equation (9) is a linear subspace, following the discussions above, we have

**Theorem 3.** *for  $m$  is even,  $\rho = 1$ , the nontrivial correlation function of the proposed sequences family  $\mathcal{V}$  takes values in  $\{-1, -1 \pm 2^{\frac{n}{2}}, -1 \pm 2^{\frac{n}{2}}\omega, -1 \pm 2^{\frac{n+e}{2}}, -1 \pm 2^{\frac{n+e}{2}}\omega\}$ .*

#### 4 Quadriphase Sequences with period $2(2^n - 1)$

Similar to the [1,2], for an even  $m$ , we propose the following sequence family, the correlation function of the sequences family is calculated.

In this section, let  $G = \{\eta_1, \eta_2, \dots, \eta_{2^n-1}\}$  be a maximum subset of  $G_C$  such that  $2\eta_i \neq 2(\eta_j + 1)$  for arbitrary  $1 \leq i, j \leq 2^n - 1$ . By convention, denote  $\beta^{\frac{1}{2}} = \beta^{2^{n-1}}$ . We present another family of quadriphase sequences with period  $2(2^n - 1)$  as follows.

**Definition 2.** A family  $\mathcal{W}$  of quadriphase sequences with period  $2(2^n - 1)$  is defined as  $\mathcal{W} = \{u_i(t), v_i(t) : 0 \leq i < 2^{n-1}\}$  is given by

1)

$$u_i(t) = \begin{cases} Tr_1^n[(1 + 2\eta_i)\beta^{t_0}] + 2P(\lambda\beta^{t_0}), t = 2t_0 \\ Tr_1^n[(1 + 2(\eta_i + 1))\beta^{t_0 + \frac{1}{2}}] + 2P(\lambda\beta^{t_0 + \frac{1}{2}}), t = 2t_0 + 1 \end{cases}$$

for  $0 \leq i < 2^{n-1}$ , where  $\eta_i \in G$ .

2)

$$v_i(t) = \begin{cases} Tr_1^n[(1 + 2\eta_i)\beta^{t_0}] + 2P(\lambda\beta^{t_0}) + 2, t = 2t_0 \\ Tr_1^n[(1 + 2(\eta_i + 1))\beta^{t_0 + \frac{1}{2}}] + 2P(\lambda\beta^{t_0 + \frac{1}{2}}), t = 2t_0 + 1 \end{cases}$$

for  $0 \leq i < 2^{n-1}$ , where  $\eta_i \in G$ .

**Theorem 4.** the correlation functions of the family  $\mathcal{W}$  satisfy the following properties. 1) if  $\tau = 2^n - 1$ , then  $R_{u_i, u_j}(\tau) = -2$ ,  $R_{v_i, v_j}(\tau) = 2$ ,  $R_{u_i, v_j}(\tau) = 0$ . 2) if  $\tau = 0$ , then  $R_{u_i, v_j}(\tau) = 0$  and

$$R_{u_i, u_j}(\tau) = R_{v_i, v_j}(\tau) = \begin{cases} 2(2^n - 1), i = j \\ -2, i \neq j, \end{cases}$$

3) If  $\tau = 2\tau_0 + 1 \neq 2^n - 1$ , then

- a)  $R_{u_i, u_j}(\tau)$  takes values in  $\{-2, -2 \pm 2^{\frac{n}{2}+1}, -2 \pm 2^{\frac{n+e}{2}+1}\}$ ,
- b)  $R_{v_i, v_j}(\tau)$  takes values in  $\{2, 2 \pm 2^{\frac{n}{2}+1}, 2 \pm 2^{\frac{n+e}{2}+1}\}$ ,
- c)  $R_{u_i, v_j}(\tau)$  takes values in  $\{\pm 2^{\frac{n}{2}+1}\omega, \pm 2^{\frac{n+e}{2}+1}\omega\}$ .

4) If  $\tau = 2\tau_0$  and  $\tau_0 \neq 0$ , then

- a)  $R_{u_i, u_j}(\tau)$  takes values in  $\{-2, -2 \pm 2^{\frac{n}{2}+1}, -2 \pm 2^{\frac{n+e}{2}+1}\}$ ,
- b)  $R_{v_i, v_j}(\tau)$  takes values in  $\{-2, -2 \pm 2^{\frac{n}{2}+1}, -2 \pm 2^{\frac{n+e}{2}+1}\}$ ,
- c)  $R_{u_i, v_j}(\tau)$  takes values in  $\{\pm 2^{\frac{n}{2}+1}\omega, \pm 2^{\frac{n+e}{2}+1}\omega\}$ .

*Proof.* In order to analysis easily, let

$$\varsigma(\gamma_1, \gamma_2, \delta) = \sum_{x \in G_C} \omega^{Tr_1^n[(1+2\gamma_1-(1+2\gamma_2)\delta)x] + 2(P(\lambda x) + P(\lambda\delta x))}. \quad (11)$$

It is easy to check that  $\varsigma(\gamma_1 + 1, \gamma_2, \delta) = \varsigma(\gamma_1, \gamma_2 + 1, \delta)^*$ , where  $*$  denotes complex conjugate.

Similar to [1], the following facts can be easily checked.

1) if  $\tau = 2\tau_0 + 1$ , then

$$\begin{aligned} R_{u_i, u_j}(\tau) &= \varsigma(\eta_i, \eta_j + 1, \delta) + \varsigma(\eta_i + 1, \eta_j, \delta) - 2, \\ R_{v_i, v_j}(\tau) &= -\varsigma(\eta_i, \eta_j + 1, \delta) - \varsigma(\eta_i + 1, \eta_j, \delta) + 2, \\ R_{u_i, v_j}(\tau) &= \varsigma(\eta_i, \eta_j + 1, \delta) - \varsigma(\eta_i + 1, \eta_j, \delta). \end{aligned}$$

2) if  $\tau = 2\tau_0$ , then

$$\begin{aligned} R_{u_i, u_j}(\tau) &= \varsigma(\eta_i, \eta_j + 1, \delta) + \varsigma(\eta_i + 1, \eta_j, \delta) - 2, \\ R_{v_i, v_j}(\tau) &= \varsigma(\eta_i, \eta_j + 1, \delta) + \varsigma(\eta_i + 1, \eta_j, \delta) - 2, \\ R_{u_i, v_j}(\tau) &= -\varsigma(\eta_i, \eta_j + 1, \delta) + \varsigma(\eta_i + 1, \eta_j, \delta). \end{aligned}$$

Due to (3),(11) and the theorem 3, the theorem 4 is proved.

Similar to the proof of the theorem 2 above, or the proof of theorem 3 and theorem 7 [1] the following theorem is obtained.

**Theorem 5.** *the linear spans of the sequences in  $\mathcal{W}$  are given as follows*

- (1) For  $u_i \in \mathcal{W}$ , the linear span  $LS(u_i)$  of  $u_i$  is given by  $LS(u_i) = \frac{n(n+e)}{2e}$ .  
(2) For  $v_i \in \mathcal{W}$ , the linear span  $LS(v_i)$  of  $v_i$  is given by  $LS(v_i) = \frac{n(n+e)}{2e} + 2$ .

## 5 Conclusions

In this paper, we have proposed the new families of quadriphase sequences with larger linear span and size. The maximum correlation magnitude of proposed sequences family is bigger than that of the related sequence in [1], and is smaller than that of the related binary sequences family in [2,3] with same parameters. The proposed two families of quadriphase sequences with period  $2^n - 1$  and  $2(2^n - 1)$  respectively for a positive integer  $n = em$  where  $m$  is an even positive can be take as an extensions of the results in [1] where  $m$  is an odd positive.

## 6 Acknowledgment

This work was supported by National Science Foundation of China under grant No.60773002 and 61072140, the Project sponsored by *SRF* for *ROCS*, *SEM*, 863 Program (2007AA01Z472), and the 111 Project (B08038).

## References

1. Jiang W.F.,Hu L.,Tang X.H.,Zeng X.Y.: New optimal quadriphase sequences with larger linear span. IEEE Trans. Inform. Theory, Vol.55, No.1, pp.458-470, Jan. 2009.
2. Tang X.H.,Udaya P.,Fan P.Z.:Generalized binary Udaya-Siddiqi sequences. IEEE Trans. Inform. Theory, Vol.53, No.3, pp.1225-1230, Mar. 2007.
3. KimS H.,No J.S.: New families of binary sequences with low cross correlation property.IEEE Trans. Inform. Theory, Vol.49, No.1, pp.3059-3065, Jan. 2009.
4. Yu N.Y.,Gong G.: A new binary sequence family with low correlation and large size. IEEE Trans. Inform. Theory, Vol.52, No.4, pp.1624-1636, Mar.2006.
5. Boztas S.,Hammons R.,Kumar P.V.: 4-phase sequences with near optimum correlation properties. IEEE Trans. Inform. Theory, Vol.14, No.3, pp.1101-1113, May 1992.

6. Kumar P.V.,Helleseeth T.,Calderbank A.R.,Hammons A.R.Jr.: Large families of quaternary sequences with low correlation. IEEE Trans. Inform. Theory, Vol.42, No.2, pp.579-592, Mar.1996.
7. Schmidt K.-U.:  $Z_4$ -valued quadratic forms and quaternary sequence families. IEEE Trans. Inform. Theory, Vol.55, No.12, pp.5803-5810, Dec.2009.
8. Sole P.: A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties.Lecture Notes in Computer Science, Vol.388, pp.193-201,1989.
9. Tang X.H.,Udaya P.:A note on the optimal quadriphase sequences families. IEEE Trans. Inform. Theory, Vol.53, No.1, pp433-436, Jan. 2007.
10. Udaya P.,Siddiqi M.U.: Optimal and suboptimal quadriphase sequences derived from maximal length sequences over  $Z_4$ .Appl. Algebra Eng. Commun.Comput., Vol.9, no.2, pp.161-191,1998.
11. Hammons A.R.Jr.,Kumar P.V.,Calderbank A.R.,Sloane N.J.A.,Sole P.: The  $Z_4$  linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inform. Theory, Vol.40, No.2, pp.301-319, Mar. 1994.
12. Tang X.T.,Udaya P.,Fan P.Z.:Quadriphase sequences obtained from binary quadratic form sequences. Lecture Note in Computer Science, Vol.3486, pp.243-254, 2005.